

PHP a MySQL – Hotová řešení

Luboslav Lacko

Většina webů se skládá z podobných komponent a funkcí, které již byly nescetněkrát naprogramovány: formuláře, přihlášení uživatele, zobrazení textových informací a grafiky, uložení a čerpání individuálních a proměnlivých informací z databáze...

Proto jsme pro vás ve spolupráci se zkušeným autorem vybrali přes dvě stovky řešení obvyklých dílčích úloh a funkčních částí, z nichž se weby různých zaměření skládají

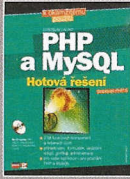
Kniha je určena především tvůrcům stránek, kteří nemají příliš zkušeností s programováním, nebo používají jiné platformy. Zachycuje již aktuální verzi PHP5.

Na příloženém CD najdete zdrojové kódy k jednotlivým řešením z knihy a software potřebný pro provozování webového serveru na Windows nebo Linuxu: PHP 5, MySQL 4 a Apache 2.

Rozsah: 304 stran

Cena: 269 Kč

Kód knihy: K0847

**Caché – Databáze postrelačního typu a tvorba aplikací**

Kolektiv autorů

Kniha začíná od prvních kroků instalace a zprovoznění systému Caché, poskytuje dobrý úvod do jeho objektově-relačních specifik, shrnuje základy objektově orientovaného programování a podává detaily o všech hlavních databázových funkcích Caché. Ukazuje programování aplikací, zejména těch webových. Najdete v ní podrobný popis objektového modelu Caché i nového Caché Studia. Prakticky zaměřené a protkané příklady jsou všechny kapitoly. Spolu se závěrečnými přehledy příkazů používaných jazyků jde o ucelenou, podrobnou příručku, která si najde – vytváříte-li aplikace v Caché – své stále místo vedle vaší klávesnice.

Rozsah: 400 stran

Cena: 490 Kč

Kód knihy: K0539

**Pasti a propasti jazyka C++**

2. aktualizované a rozšířené vydání

Miroslav Virius

Pojďte poznat nejčastější chyby, jichž se dopouštějí programátoři v C++, pod vedením odborníka nad jiné zkušeného, který nástrahy a pasti jazyka od těch, kdo v nich uvízli, sbírá již dvě desetiletí. Náhorně vám je předvede a objasní, abyste do nich sami neupadli. Nejedná se o jednoduché algoritmické ani syntaktické chyby, ale o problémy, které mají na svědomí méně známá pravidla jazyků C a C++, podobnost s jinými programovacími jazyky (hlavně s Pascalem a Javou) nebo běžné překlepy – tedy konstrukce, které překladač i program provede, ale pravděpodobně jinak, než jeho tvůrce zamýšlel.

Rozsah: 376 stran

Cena: 349 Kč

Kód knihy: K1049



Security holes 04/05

13. komnata

ARJ dělá problémy

Hned dva výrobci v poslední době oznámili problémy se svými produkty při práci s archivy formátu ARJ. Předně antivirový software Trend Micro špatně zachází s hlavičkou souboru, což na neopravených systémech může pomoci chyby přetečení bufferu vyústit ve spuštění cizího kódu. Také konkurenční software F-Secure se nedávno potýkal s problémy při otvírání ARJ, zde bylo oznámení vydáno přibližně v polovině února.

www.trendmicro.comwww.f-secure.com/security/fsc-2005-1.shtml**MD5: nikoli zda, ale jak rychle**

O průlomu hashovací funkce MD5 jsme psali v době, kdy byla tato událost nová. Otázka již dávno nezní zda, už se řeší jen jak rychle. Známy český kryptolog Vlastimil Klíma našel zlepšení, které hledá kolize 3–6× rychleji než původní metoda. Podle materiálů trvalo nalezení kolize na běžném notebooku 8 h. Znovu opakujeme, že jakékoli

systémy, založené na jednoduše této hashovací funkce, již nějakou dobu nejsou absolutně bezpečné, protože tento základní požadavek obtížnosti reverzního výpočtu prostě nemají.

cryptography.hyperlink.cz/md5/md5_collisions.pdf

Real problem

Přestože hudební produkty od Real Networks nejsou v našich končinách dominantně rozšířeny, informujeme o vážném problému RealPlayeru, jehož působnost jde přes všechny platformy – Windows, Linux i Mac. Objevily se zásadní nedostatky ve zpracování některých souborů (různá oznámení mluví o smil a waw), které mohou vyvolat spuštění dat a tím de facto nést spustitelný kód jako jakýkoli jiný skutečně „executable“ soubor. Ze strany uživatele je nutná interakce pouze v podobě otevření souboru (RealPlayerem). Konkrétní postižené aplikace si můžete najít v oznámení.

www.idefense.com/application/poi/display?id=209

Někdy se stačí jen zeptat

Google je oblíbený především díky své schopnosti vracet přesné výsledky, které sesbíral skutečně „po všech koutech“. Pokud se umíme dobře zeptat, můžeme dostat i velmi cenné informace, které nemusí být pro veřejnost určeny. Speciálně u programů, které generují výstup v HTML.

Klasickým příkladem může být BigBrother. Jeho uživatelské rozhraní je speciálně vhodné pro indexování vyhledávačem. Pokud jste administrátor unixových/linuxových serverů, možná vám není cizí. Dokáže monitorovat stavy různých zařízení, jako například dostupnost http, ftp, pop3 apod. Tedy informace relativně důležité.

Hlavním přínosem programu je fakt, že všechny důležité informace jsou ihned vidět na jedné webové stránce. Pokud spravujete více serverů, tento produkt vám umožní okamžitě získat přehled o všech z nich navštívením jednoho webu, což je docela užitečné. Status „vše v pořádku“ systém indikuje zelenou barvou, zásadní problémy pak červeně.

Celkový status navíc vidíte v záhlaví okna prohlížeče: pokud je někde červený alert, bude mít okno titulek red:Big Brother.

Administrátoři obvykle monitorují zásadní „jev“, které mohou na serveru nastat. Když máte webserver, tak vás určitě zajímají položky http a conn, protože se chcete ujistit, že se lidé stále mohou k vašemu serveru připojit. Ale existuje spousta dalších testů, např. monitorování Oracle databáze či seznamu připojených uživatelů apod.

Kde je problém?

Ocitujme dvě věci z oficiálního BB4 Technologies FAQ – Section 5: Security Considerations (bb4.com/bb/help/bb-faq.html#5.0): „BB nepotřebuje běžet jako root. Doporučujeme vytvořit uživatele „bb“ a program nechat běžet pod ním“ a „Doporučujeme zabezpečit výstupní stránky BB heslem.“

Hned víme, že administrátoři budou mít BB spuštěný nejspíše pod uživatelem „bb“, který ovšem může mít také rootovská práva. To dává útočníkovi ihned jeden funkční účet. Jelikož se patrně často nepoužívá, může mít nějaké slabší heslo. Druhá věc je, že nezaheslované stránky jsou vidět. Roboti různých vyhledávacích enginů je určitě také prošli a rádi vám